

P/2371-27

JCS11 U.S. PTO
09/437924



日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

出願書中の記載されている事項は下記の出願書類に記載されて
いることを証明する。

This is to certify that the annexed is a true copy of the following application as filed

Application: 1998年11月12日

特許番号: 平成10年特許願第336474号

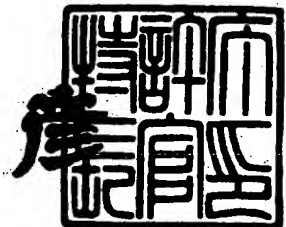
出願人: 日本電気株式会社

PRIORITY DOCUMENT
CERTIFIED COPY OF

1999年 9月17日

特許庁長官
Commissioner,
Patent Office

近藤 隆



出証番号 出証特平11-3063586

【書類名】 特許願

【整理番号】 63110992

【提出日】 平成10年11月12日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/22

【発明の名称】 認証管理システム及び認証管理方法

【請求項の数】 14

【発明者】

 【住所又は居所】 東京都港区芝五丁目7番1号
日本電気株式会社内

 【氏名】 広瀬 隆

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

 【代表者】 金子 尚志

【代理人】

 【識別番号】 100097113

 【弁理士】

 【氏名又は名称】 堀 城之

 【電話番号】 03(5512)7377

【手数料の表示】

 【予納台帳番号】 044587

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9708414

【書類名】 明細書

【発明の名称】 認証管理システム及び認証管理方法

【特許請求の範囲】

【請求項 1】 コンピュータ等を使用した電子文書の認証管理システムであって、

コンピュータ等を使用した電子文書及び／または電子文書の印字結果に表示される認証としての印章及び／またはサインイメージに、当該認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記する手段と、

文書に対する認証の根拠と成り得る管理番号及び／または保管システムのコードを当該電子文書中にバーコード形式で付記する手段とを有する

ことを特徴とする認証管理システム。

【請求項 2】 コンピュータ等を使用した電子文書の認証管理システムであって、

コンピュータ等を使用した電子文書を、当該電子文書の文章承認者に対する認証の根拠と成り得る認証データ及び当該文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、前記電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データを生成する電子文章データ保管システムと、

個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、当該個人や法人からの要求に応じて、当該要求のあった認証データ及び当該認証データに対する認証の根拠と成り得る管理番号を前記電子文章データ保管システムに送付する認証データ保管システムとを有する

ことを特徴とする認証管理システム。

【請求項 3】 コンピュータ等を使用した電子文書の認証管理システムであって、

認証手段としての印章及び／またはサインイメージの近傍であって当該印章及び／またはサインイメージの真贋の確認が容易な位置に、当該印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／また

は保管機関のコードをバーコード形式で付記して前記電子文書を保管する電子文章データ保管システムと、

個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データとして保管する認証データ保管システムとを有し、

前記電子文章データ保管システムと前記認証データ保管システムとは、相互に前記認証データの管理番号と文章管理番号を保管及び管理する

ことを特徴とする認証管理システム。

【請求項 4】 前記電子文章データ保管システムは、接続された前記コンピュータシステムの特定されたユーザーから前記電子文章データを安全に送受信する機能を有する

ことを特徴とする請求項 2 または 3 に記載の認証管理システム。

【請求項 5】 前記電子文章データ保管システムは、前記電子文章データを保管し、当該電子文章データから必要な認証者を読み出し、通信手段を用いて認証者の承認を得て、前記認証データ保管システムから前記認証データを受け取る機能を有する

ことを特徴とする請求項 2 乃至 4 のいずれか一項に記載の認証管理システム。

【請求項 6】 前記認証データ保管システムは、認証者から受け取った前記認証データを保管管理する機能を有する

ことを特徴とする請求項 2 乃至 5 のいずれか一項に記載の認証管理システム。

【請求項 7】 前記認証データ保管システムは、前記電子文章データ保管システムとの間でネットワークを介して取得する前記電子文章データからの認証データ要求に対応して、認証者のコンピュータシステムと通信手段とにより承認を取り、管理番号付きの前記認証データを送付する機能を有する

ことを特徴とする請求項 6 に記載の認証管理システム。

【請求項 8】 コンピュータ等を使用した電子文書の認証管理方法であって

コンピュータ等を使用した電子文書及び／または電子文書の印字結果に表示される認証としての印章及び／またはサインイメージに、当該認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記する工程と、

文書に対する認証の根拠と成り得る管理番号及び／または保管システムのコードを当該電子文書中にバーコード形式で付記する工程とを有する

ことを特徴とする認証管理方法。

【請求項 9】 コンピュータ等を使用した電子文書の認証管理方法であって

、
コンピュータ等を使用した電子文書を、当該電子文書の文章承認者に対する認証の根拠と成り得る認証データ及び当該文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、前記電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データを生成する電子文章データ保管工程と、

個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、当該個人や法人からの要求に応じて、当該要求のあった認証データ及び当該認証データに対する認証の根拠と成り得る管理番号を前記電子文章データ保管工程に送付する認証データ保管工程とを有する

ことを特徴とする認証管理方法。

【請求項 10】 コンピュータ等を使用した電子文書の認証管理方法であって、

認証工程としての印章及び／またはサインイメージの近傍であって当該印章及び／またはサインイメージの真贋の確認が容易な位置に、当該印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／または保管機関のコードをバーコード形式で付記して前記電子文書を保管する電子文章データ保管工程と、

個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データとして保管する認証データ保管工程とを有し、

前記電子文章データ保管工程と前記認証データ保管工程とは、相互に前記認証データの管理番号と文章管理番号を保管及び管理する

ことを特徴とする認証管理方法。

【請求項 11】 前記電子文章データ保管工程は、接続された前記コンピュ

ータシステムの特定されたユーザーから前記電子文章データを安全に送受信する工程を有する

ことを特徴とする請求項 9 または 10 に記載の認証管理方法。

【請求項 12】 前記電子文章データ保管工程は、前記電子文章データを保管し、当該電子文章データから必要な認証者を読み出し、通信工程を用いて認証者の承認を得て、前記認証データ保管工程から前記認証データを受け取る工程を有する

ことを特徴とする請求項 9 乃至 11 のいずれか一項に記載の認証管理方法。

【請求項 13】 前記認証データ保管工程は、認証者から受け取った前記認証データを保管管理する工程を有する

ことを特徴とする請求項 9 乃至 12 のいずれか一項に記載の認証管理方法。

【請求項 14】 前記認証データ保管工程は、前記電子文章データ保管工程との間でネットワークを介して取得する前記電子文章データからの認証データ要求に対応して、認証者のコンピュータシステムと通信工程とにより承認を取り、管理番号付きの前記認証データを送付する工程を有する

ことを特徴とする請求項 13 に記載の認証管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、認証技術に関し、特に、コンピュータ使用の電子文書の認証管理システム及び認証管理方法に関する。

【0002】

【従来の技術】

近年、コンピュータ等を使用した電子文書及び電子文書の印字結果に表示される認証としての印章やサインイメージの真贋の確認が容易な印字及び表示方式が求められている。そして、認証データと電子文書を各々別々にかつ関連づけて、確認容易な形態で保管すること、ネットワークを活用したオープン性に富みかつ信頼性の高い認証管理システム及び認証管理方法が求められている。

【0003】

このようなコンピュータ使用の電子文書の認証管理システム及び認証管理方法としては、例えば、特開平6-119363号公報に記載の技術が開示されている（従来技術）。従来技術の電子文書承認方式は、ワードプロセッサや電子メールの文書を扱うコンピュータシステムの電子文書承認方式において、作成された電子文書データを記憶する文書データ記憶手段と、承認者の印章やサインをイメージデータとして承認者番号と対応して記憶する承認イメージ手段と、文書データ記憶手段に記憶されている電子文書データのデータ変更を不可とする書込み保護属性をその電子文書データに付加する書込み保護属性付加手段と、承認者の操作により文書データ記憶手段に記憶されている電子文書データに承認者番号を含む承認情報を付加し、書込み保護属性付加手段を介して書込み保護属性を付加させる承認情報付加手段と、文書データ記憶手段が記憶している承認情報付加手段が承認情報および書込み保護属性を付加した電子文書データを承認者番号の指定により読出し、承認イメージデータ記憶手段に記憶している承認者番号に対応するイメージデータを読出した電子文書データに合成して出力装置に出力する合成出力手段とを有することにより構成される。更に、コンピュータによるワードプロセッサや電子メールの電子文書の承認において、承認イメージデータを持ち、出力時に合成して出力すること、および承認者の操作により文書データに承認情報を付加することにより文書データの変更を不可とすることができる結果、承認する資格のない人間による不正な承認を防ぐことができ、また、承認後の不正な変更を防ぐことができ、電子文書を、犯罪、不正行為などの人間の悪意による意図的行為から保護することができる効果があることが述べられている。

【0004】

【発明が解決しようとする課題】

しかしながら、従来技術は、印字された認証データ部だけでは認証データの確認が容易ではないため、その認証データの真贋の判定が困難であるという問題点があった。

【0005】

更に、独立したシステム環境が構築されておらず、認証データ保管システムに文章データ管理番号が送られないため、印字された認証データに個々の使用番号

が記憶されない。その結果、認証データから個々の文章データを検索できず、オープンなシステムとして文章管理や認証データ管理ができないという問題点もあった。

【0006】

本発明は斯かる問題点を鑑みてなされたものであり、その目的とするところは、コンピュータ等を使用した電子文書及び電子文書の印字結果に表示される認証としての印章やサインイメージの真贋の確認が容易な印字及び表示ができるとともに、認証データと電子文書を各々別々にかつ関連づけて確認容易な形態で保管できるオープン性に富みかつ信頼性の高い認証管理システム及び認証管理方法を提供する点にある。

【0007】

【課題を解決するための手段】

本発明の要旨は、コンピュータ等を使用した電子文書の認証管理システムであって、コンピュータ等を使用した電子文書及び／または電子文書の印字結果に表示される認証としての印章及び／またはサインイメージに、当該認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記する手段と、文書に対する認証の根拠と成り得る管理番号及び／または保管システムのコードを当該電子文書中にバーコード形式で付記する手段とを有することを特徴とする認証管理システムに存する。

また本発明の請求項2に記載の要旨は、コンピュータ等を使用した電子文書の認証管理システムであって、コンピュータ等を使用した電子文書を、当該電子文書の文章承認者に対する認証の根拠と成り得る認証データ及び当該文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、前記電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データを生成する電子文章データ保管システムと、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、当該個人や法人からの要求に応じて、当該要求のあった認証データ及び当該認証データに対する認証の根拠と成り得る管理番号を前記電子文章データ保管システムに送付する認証データ保管システムとを

有することを特徴とする認証管理システムに存する。

また本発明の請求項 3 に記載の要旨は、コンピュータ等を使用した電子文書の認証管理システムであって、認証手段としての印章及び／またはサインイメージの近傍であって当該印章及び／またはサインイメージの真贋の確認が容易な位置に、当該印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／または保管機関のコードをバーコード形式で付記して前記電子文書を保管する電子文章データ保管システムと、個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データとして保管する認証データ保管システムとを有し、前記電子文章データ保管システムと前記認証データ保管システムとは、相互に前記認証データの管理番号と文章管理番号を保管及び管理することを特徴とする認証管理システムに存する。

また本発明の請求項 4 に記載の要旨は、前記電子文章データ保管システムは、接続された前記コンピュータシステムの特定されたユーザーから前記電子文章データを安全に送受信する機能を有することを特徴とする請求項 2 または 3 に記載の認証管理システムに存する。

また本発明の請求項 5 に記載の要旨は、前記電子文章データ保管システムは、前記電子文章データを保管し、当該電子文章データから必要な認証者を読み出し、通信手段を用いて認証者の承認を得て、前記認証データ保管システムから前記認証データを受け取る機能を有することを特徴とする請求項 2 乃至 4 のいずれか一項に記載の認証管理システムに存する。

また本発明の請求項 6 に記載の要旨は、前記認証データ保管システムは、認証者から受け取った前記認証データを保管管理する機能を有することを特徴とする請求項 2 乃至 5 のいずれか一項に記載の認証管理システムに存する。

また本発明の請求項 7 に記載の要旨は、前記認証データ保管システムは、前記電子文章データ保管システムとの間でネットワークを介して取得する前記電子文章データからの認証データ要求に対応して、認証者のコンピュータシステムと通信手段とにより承認を取り、管理番号付きの前記認証データを送付する機能を有することを特徴とする請求項 6 に記載の認証管理システムに存する。

また本発明の請求項 8 に記載の要旨は、コンピュータ等を使用した電子文書の認証管理方法であって、コンピュータ等を使用した電子文書及び／または電子文書の印字結果に表示される認証としての印章及び／またはサインイメージに、当該認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記する工程と、文書に対する認証の根拠と成り得る管理番号及び／または保管システムのコードを当該電子文書中にバーコード形式で付記する工程とを有することを特徴とする認証管理方法に存する。

また本発明の請求項 9 に記載の要旨は、コンピュータ等を使用した電子文書の認証管理方法であって、コンピュータ等を使用した電子文書を、当該電子文書の文章承認者に対する認証の根拠と成り得る認証データ及び当該文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、前記電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データを生成する電子文章データ保管工程と、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、当該個人や法人からの要求に応じて、当該要求のあった認証データ及び当該認証データに対する認証の根拠と成り得る管理番号を前記電子文章データ保管工程に送付する認証データ保管工程とを有することを特徴とする認証管理方法に存する。

また本発明の請求項 10 に記載の要旨は、コンピュータ等を使用した電子文書の認証管理方法であって、認証工程としての印章及び／またはサインイメージの近傍であって当該印章及び／またはサインイメージの真贋の確認が容易な位置に、当該印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／または保管機関のコードをバーコード形式で付記して前記電子文書を保管する電子文章データ保管工程と、個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データとして保管する認証データ保管工程とを有し、前記電子文章データ保管工程と前記認証データ保管工程とは、相互に前記認証データの管理番号と文章管理番号を保管及び管理することを特徴とする認証管理方法に存する。

また本発明の請求項 11 に記載の要旨は、前記電子文章データ保管工程は、接続された前記コンピュータシステムの特定されたユーザーから前記電子文章データを安全に送受信する工程を有することを特徴とする請求項 9 または 10 に記載の認証管理方法に存する。

また本発明の請求項 12 に記載の要旨は、前記電子文章データ保管工程は、前記電子文章データを保管し、当該電子文章データから必要な認証者を読み出し、通信工程を用いて認証者の承認を得て、前記認証データ保管工程から前記認証データを受け取る工程を有することを特徴とする請求項 9 乃至 11 のいずれか一項に記載の認証管理方法に存する。

また本発明の請求項 13 に記載の要旨は、前記認証データ保管工程は、認証者から受け取った前記認証データを保管管理する工程を有することを特徴とする請求項 9 乃至 12 のいずれか一項に記載の認証管理方法に存する。

また本発明の請求項 14 に記載の要旨は、前記認証データ保管工程は、前記電子文章データ保管工程との間でネットワークを介して取得する前記電子文章データからの認証データ要求に対応して、認証者のコンピュータシステムと通信工程とにより承認を取り、管理番号付きの前記認証データを送付する工程を有することを特徴とする請求項 13 に記載の認証管理方法に存する。

【0008】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【0009】

(第 1 実施形態)

図 1 は、本発明の認証管理システムの一実施形態を示す機能ブロック図である。図 1 に示すように、本実施形態の認証管理システムは、ネットワーク 60 に相互に安全性をもって通信可能に接続された任意の数のコンピュータシステム 10、50、ネットワーク 60 上に相互に安全に通信可能に接続された任意の数の電子文章データ保管システム 20、任意の数の認証データ保管システム 30、40 を有している。

【0010】

コンピュータシステム10, 50は、電子文章データ1を作成するワープロ機能、パスワードなど安全性を有した通信手段で電子文章データ1の送信や受信を実行する通信機能、認証データ3, 4の送信や受信を実行する認証機能、バーコード等のイメージデータを印字する出力機能を有する。

【0011】

本実施形態の電子文章データ保管システム20は、電子文章データ保管工程を実行する手段であって、コンピュータ等を使用した電子文書を、この電子文書の文章承認者に対する認証の根拠と成り得る認証データ及びこの文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データ1を生成する。

【0012】

換言すれば、電子文章データ保管システム20は、認証手段としての印章及び／またはサインイメージの近傍であってこの印章及び／またはサインイメージの真贋の確認が容易な位置に、この印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号3-3, 4-3をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／または保管機関のコードをバーコード形式で付記して電子文書を保管する。

【0013】

また電子文章データ保管システム20は、接続されたコンピュータシステム10, 50の特定されたユーザーから電子文章データ1を安全に送受信する機能、電子文章データ1を保管し、その電子文章データ1から必要な認証者を読み出し、通信手段を用いて認証者の承認を得て、認証データ保管システム30, 40から認証データ3, 4を受け取る機能を有する。

【0014】

本実施形態の認証データ保管システム30, 40は、認証データ保管工程を実行する手段であって、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、この個人や法人からの要求に応じて、この要求のあった認証データ及びこの認証データに対する認証の根拠と成

り得る管理番号を電子文章データ保管システム20に送付する。

【0015】

換言すれば、認証データ保管システム30、40は、個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データ3，4として保管する。

【0016】

このような電子文章データ保管システム20と認証データ保管システム30、40とは、相互に認証データ3，4の管理番号と文章管理番号を保管及び管理する。

【0017】

また認証データ保管システム30、40は、認証者から受け取った認証データ3，4を保管管理するとともに、電子文章データ保管システム20との間でネットワーク60を介して取得する電子文章データ1からの認証データ要求に対応して、認証者のコンピュータシステム10，50と通信手段とにより承認を取り、管理番号付きの認証データ3，4を送付する機能を有する。

【0018】

続いて、本実施形態の認証管理システムの動作を説明する。

【0019】

コンピュータシステム10を用いて電子文章データ1を作成し、電子文章データ保管システム20に自らの承認データを添付して保管すると、この承認データの保管に応じて、電子文章データ保管システム20は、認証データ保管システム30、40に必要認証者の認証データ3，4を要求する。

【0020】

この認証データ3，4を要求に応じて、各認証データ保管システム30、40は、電子文章データ保管システム20から文書データ管理番号を受け取って仮保管し、各認証者の承認を得て、電子文章データ保管システム20に認証データ3，4と管理番号を送付する。

【0021】

この認証データ3，4と管理番号の送付に応じて、認証データ保管システム3

0、40は、文書データ管理番号を保管する。

【0022】

これに応じて、電子文章データ保管システム20は、各認証データ3、4を収集後、電子文書の中に認証データ3、4とその管理番号、電子文章データ保管システム20の管理番号を記入し、その管理番号をバーコードにて表示し、電子文章データ1として保管し、各認証者のコンピュータシステム10、50にその電子文章データ1を送信する。

【0023】

この電子文章データ1の送信に応じて、受信した各コンピュータシステム10、50は、その電子文章データ1を保管、印字を行う。

【0024】

次に、本実施形態の認証管理システムにおいて、図2に示す電子文章データ1が作成された過程について説明する。図2は、図1の認証管理システムで用いられる電子文章データ1の印字結果の概略構成を示している。

【0025】

図2に示す電子文章データ1は、電子文章データ保管システム20に保管され、そのシステムを特定する管理番号とそのバーコード2、文書管理の文書番号とそのバーコード1-1、認証者の認証データ3、4を文書内に有している。また電子文章データ1には、文書名1-2の場所に題名が、文1-3の場所に文の内容が記載されるようになっている。

【0026】

認証データ3は、認証イメージデータ3-1、認証データ保管システム30の管理番号と認証者の管理番号3-2、使用番号3-3、及びこれらの各々のバーコードを有している。

【0027】

認証データ4は、認証イメージデータ4-1、認証データ保管システム40の管理番号と認証者の管理番号4-2、使用番号4-3、及びこれらの各々のバーコードを有している。

【0028】

図3は、本発明の認証管理方法を用いた文書作成手順の一実施形態を示すフローチャートである。本実施形態の認証管理方法は、コンピュータ等を使用した電子文書の認証管理方法であって、コンピュータ等を使用した電子文書及び／または電子文書の印字結果に表示される認証としての印章及び／またはサインイメージに、この認証の根拠と成り得る管理番号及び／または使用番号をバーコード形式で付記する工程と、文書に対する認証の根拠と成り得る管理番号及び／または保管システムのコードをこの電子文書中にバーコード形式で付記する工程とを実行するために、電子文章データ保管工程、認証データ保管工程を有している。

【0029】

電子文章データ保管工程は、図3に示すように、電子文章データ保管システム20が実行する工程であって、コンピュータ等を使用した電子文書を、この電子文書の文章承認者に対する認証の根拠と成り得る認証データ及びこの文章承認者に対する認証の根拠と成り得る認証データの管理番号とともに承認データの受付時の状態で保管し、電子文書に対する認証の根拠と成り得る電子文章管理番号に基づく認証データを追加した電子文章データ1を生成する。

【0030】

換言すれば、電子文章データ保管工程は、認証工程としての印章及び／またはサインイメージの近傍であってこの印章及び／またはサインイメージの真贋の確認が容易な位置に、この印章及び／またはサインイメージに対する認証の根拠と成り得る管理番号及び／または使用番号3-3, 4-3をバーコード形式で付記するとともに、印字文書の中に文書の管理番号及び／または保管機関のコードをバーコード形式で付記して電子文書を保管する。

【0031】

このような電子文章データ保管工程は、接続されたコンピュータシステム10, 50の特定されたユーザーから電子文章データ1を安全に送受信する工程を有し、電子文章データ1を保管し、この電子文章データ1から必要な認証者を読み出し、通信工程を用いて認証者の承認を得て、認証データ保管工程から認証データ3, 4を受け取る工程を有する。

【0032】

一方、認証データ保管工程は、図3に示すように、認証データ保管システム30、40が実行する工程であって、個人や法人に対する認証の根拠と成り得る印章やサインなどのイメージデータを認証データとして保管し、この個人や法人からの要求に応じて、この要求のあった認証データ及びこの認証データに対する認証の根拠と成り得る管理番号を電子文章データ保管工程に送付する。

【0033】

換言すれば、認証データ保管工程は、個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データ3、4として保管する。

【0034】

このような電子文章データ保管工程と認証データ保管工程とは、相互に認証データ3、4の管理番号と文章管理番号を保管及び管理する。

【0035】

このような認証データ保管工程は、認証者から受け取った認証データ3、4を保管管理する工程を有し、電子文章データ保管工程との間でネットワーク60を介して取得する電子文章データ1からの認証データ要求に対応して、認証者のコンピュータシステム10、50と通信工程とにより承認を取り、管理番号付きの認証データ3、4を送付する工程を有する。

【0036】

次に、電子文章データ1の作成手順を図3を用いて説明する。電子文章データ1が図2に示す甲と乙の2人が承認する書類（契約書等を含む）の場合であって、認証者の一人である“甲”（図2、図3に示す”中山“氏）がコンピュータシステム10を使用して、電子文章データ1を作成するケースについて説明する。

【0037】

”中山“氏が、コンピュータシステム10を使用して認証者の認証管理番号の付いた電子文章の仮データを作成する。ここで、仮データと称するのは、電子文章データ保管システム20の管理番号や文書番号、認証データ3、4をまだ含んでいないからである。

【0038】

コンピュータシステム 10 は、電子文章データ保管システム 20 にこの電子文章の仮データを送信するとともに、この電子文章データ保管システム 20 から文書管理番号を取得する。

【0039】

電子文章データ保管システム 20 は、取得した文書管理番号を文書管理ファイル 21 に仮保管する。

【0040】

電子文章データ保管システム 20 は、電子文章データ 1 中の必要な認証者の認証管理番号に基づいて、認証データ保管システム 30、40 の各々に認証データ 3、4 を要求する。認証データ保管システム 30、40 の各々に認証データ 3、4 を要求する場合、電子文章データ保管システム 20 は、システムの管理番号、文書管理番号、及び仮の電子文章データ 1 を送信する。

【0041】

要求順序は、作成者の認証データ 3、4 に基づいて求める。認証データ 3、4 を要求された各認証データ保管システム 30、40 は、電子文章データ 1 の仮文書を添付して各認証者に承認を求める。

【0042】

電子文章データ保管システム 20 は、認証データ保管システム 30 を通して “甲 “に該当する” 中山 “氏の承認に応じて、認証データ保管システム 30 から認証データ 3 を入手し、認証データ保管システム 40 を介して “乙 “に該当する” 田中 “氏の承認を得ることにより、認証データ保管システム 40 から認証データ 4 を入手する。

【0043】

各認証データ保管システム 30、40 は、認証管理ファイル 31、41 の各々に保管されている各々の認証者の管理番号に対応させて、使用番号 3-3、4-3、及び電子文章データ保管システム 20 の管理番号と文書の管理番号を関連づけて保管する。

【0044】

認証データ 3 は、認証イメージデータ 3-1、認証データ保管システム 30 の

管理番号と認証者の管理番号 3-2、使用番号 3-3、及びこれらの各々のバーコードを有している。

【0045】

認証データ 4 は、認証イメージデータ 4-1、認証データ保管システム 40 の管理番号と認証者の管理番号 4-2、使用番号 4-3、及びこれらの各々のバーコードを有している。

【0046】

電子文章データ保管システム 20 は、最終的な電子文章データ 1 を完成し、保護された状態で文書管理ファイル 21 に保管する。

【0047】

この電子文章データ 1 の内容を確認することが許可された、特定の人もしくは一般の人はコンピュータシステム 10、50 からこの電子文章データ保管システム 20 にアクセスすることにより、電子文章データ 1 を入手し、印字することが可能となる。

【0048】

以上第 1 実施形態を要約すれば、認証としての印章及び／またはサインイメージの真贋の確認が容易なように認証としての印章及び／またはサインイメージの近傍にその認証の根拠と成り得る管理番号及び／または使用番号 3-3、4-3 を数字とバーコード形式で付記するとともに印字文書の中に文書の管理番号及び／または保管機関のコードを数字とバーコード形式で付記し、バーコードリーダーを持つコンピュータシステム 10、50 にてチェックすることにより、迅速に認証データ 3、4 や電子文章データ 1 を検索し、各保管システムから取り出すことができるようになる。その結果、電子文章データ 1 に含まれる、認証データ 3、4 から容易に認証データ保管システム 30、40 を割り出せ、アクセスすることにより認証データ 3、4 の真贋を容易に判定でき、また、電子文章データ 1 をも検索し易いというメリットを有する。

【0049】

更に、認証データ 3、4 を必要とする電子文章データ 1 を保管する電子文章データ保管システム 20 と個人及び／または法人に対する認証の根拠と成り得る印

章やサインを含むイメージデータを認証データ 3, 4 として保管する認証データ保管システム 30、40 を独立したシステムとして構成し、これをネットワーク 60 で認証者のコンピュータシステム 10、50 と、及び、認証データ保管システム 30、40 相互に接続することにより、電子文章データ 1 の作成者が、作成した仮の電子文章データ 1 を一旦、電子文章データ保管システム 20 に保管し、電子文章データ保管システム 20 が認証データ保管システム 30、40 を介して認証データ 3, 4 を得るとともに相互に認証データ 3, 4 の管理番号と文章管理番号を保管及び管理することができるようになる。その結果、電子文章データ保管システム 20 と認証データ保管システム 30、40 が各々、独立したシステムとなっており、安全性に富んだ、オープンなシステムを構成できるようになる。

【0050】

(第 2 実施形態)

本実施形態の認証管理システムは、電子文章の仮データの作成時に、作成者が自らの認証データ 3, 4 を認証データ保管システム 30、40 から仮入手する。このとき、認証データ保管システム 30、40 には、電子文章データ保管システム 20 の管理番号や文章番号は与えられず、認証データ 3, 4 の仮使用番号が送信される。

【0051】

電子文章データ保管システム 20 に仮文章データが送信された後、作成者の承認を得ることなく、電子文章データ保管システム 20 と認証データ保管システム 30、40 間で管理番号や文書番号の送信を行う。この場合、承認手続きが一部省力できるといったメリットを有する。

【0052】

以上第 2 実施形態を要約すれば、認証としての印章及び／またはサインイメージの真贋の確認が容易なように認証としての印章及び／またはサインイメージの近傍にその認証の根拠と成り得る管理番号及び／または使用番号 3-3, 4-3 を数字とバーコード形式で付記するとともに印字文書の中に文書の管理番号及び／または保管機関のコードを数字とバーコード形式で付記し、バーコードリーダーを持つコンピュータシステム 10、50 にてチェックすることにより、迅速に

認証データ 3, 4 や電子文章データ 1 を検索し、各保管システムから取り出すことができるようになる。その結果、電子文章データ 1 に含まれる認証データ 3, 4 から容易に認証データ保管システム 30、40 を割り出せ、アクセスすることにより認証データ 3, 4 の真贋を容易に判定でき、また、電子文章データ 1 をも検索し易いというメリットを有する。

【0053】

更に、認証データ 3, 4 を必要とする電子文章データ 1 を保管する電子文章データ保管システム 20 と個人及び／または法人に対する認証の根拠と成り得る印章やサインを含むイメージデータを認証データ 3, 4 として保管する認証データ保管システム 30、40 を独立したシステムとして構成し、これをネットワーク 60 で認証者のコンピュータシステム 10、50 と、及び、認証データ保管システム 30、40 を相互に接続することにより、電子文章データ 1 の作成者が、作成した仮の電子文章データ 1 を一旦、電子文章データ保管システム 20 に保管し、電子文章データ保管システム 20 が認証データ保管システム 30、40 を介して認証データ 3, 4 を得るとともに相互に認証データ 3, 4 の管理番号と文章管理番号を保管及び管理することができるようになる。その結果、電子文章データ保管システム 20 と認証データ保管システム 30、40 が各々、独立したシステムとなっており、安全性に富んだ、オープンなシステムを構成できるようになる。

【0054】

なお、本実施の形態においては、本発明は電子文章データに限定されず、本発明を適用する上で好適な電子マネー (Electronic Money, Digital Cash) に対する認証技術、クレジットカードに対する認証技術、電子商取引 (エレクトロニック・コマース: Electronic Commerce) に対する認証技術、電子銀行システム (エレクトロニック・バンキング: Electronic Banking) に対する認証技術等に広く適用することができる。また、上記構成部材の数、位置、形状等は上記実施の形態に限定されず、本発明を実施する上で好適な数、位置、形状等にすることができる。また、各図において、同一構成要素には同一符号を付している。

【0055】

【発明の効果】

本発明は、認証としての印章やサインイメージの真贋の確認が容易なように認証としての印章やサインイメージの近傍にその認証の管理番号及び使用番号をバーコード形式で付記するとともに印字文書の中に文書の管理番号及び保管機関のコードをバーコード形式で付記し、オープン性に富みかつ信頼性の高い認証管理システム及び認証管理方法の実現のため電子文書を保管する電子文章データ保管システムと個人や法人の印章やサインなどのイメージデータを認証データとして保管する認証データ保管システムにおいて、相互に認証データの管理番号と文章管理番号を保管及び管理する。

【0056】

これにより、電子文章データ保管システムと認証データ保管システムの両方の管理システムに通信的に接続されたコンピュータのバーコードリーダーを用いて認証データの下のバーコードを読みとることにより、認証データ保管システムからその文章データを承認したかどうかの確認が取れるようになる。また文章データの管理番号のバーコードを読みとり、電子文章データ保管システムからその文章が正しいことを確認できる。その結果、コンピュータ等を使用した電子文書及び電子文書の印字結果に表示される認証としての印章やサインイメージの真贋の確認が容易な印字及び表示ができるようになり、セキュリティ性の向上を図ることができるといった効果を奏する。

【0057】

また、認証データに管理番号のバーコードを追加することにより、電子文書及び電子文書の印字結果に表示される認証としての印章やサインイメージの真贋の確認が容易になるといった効果を奏する。

【0058】

更に、認証データと文章データに管理番号を付けるとともに相互に保管管理することにより、認証データと電子文書を各々別々にかつ関連づけて確認容易な形態で保管できるようになる。その結果、高いオープン性と高い信頼性とを両立できるといった効果を奏する。

【図面の簡単な説明】

【図 1】

本発明の認証管理システムの一実施形態を示す機能ブロック図である。

【図 2】

図 1 の認証管理システムで用いられる電子文章データの印字結果の概略構成を示している。

【図 3】

本発明の認証管理方法を用いた文書作成手順の一実施形態を示すフローチャートである。

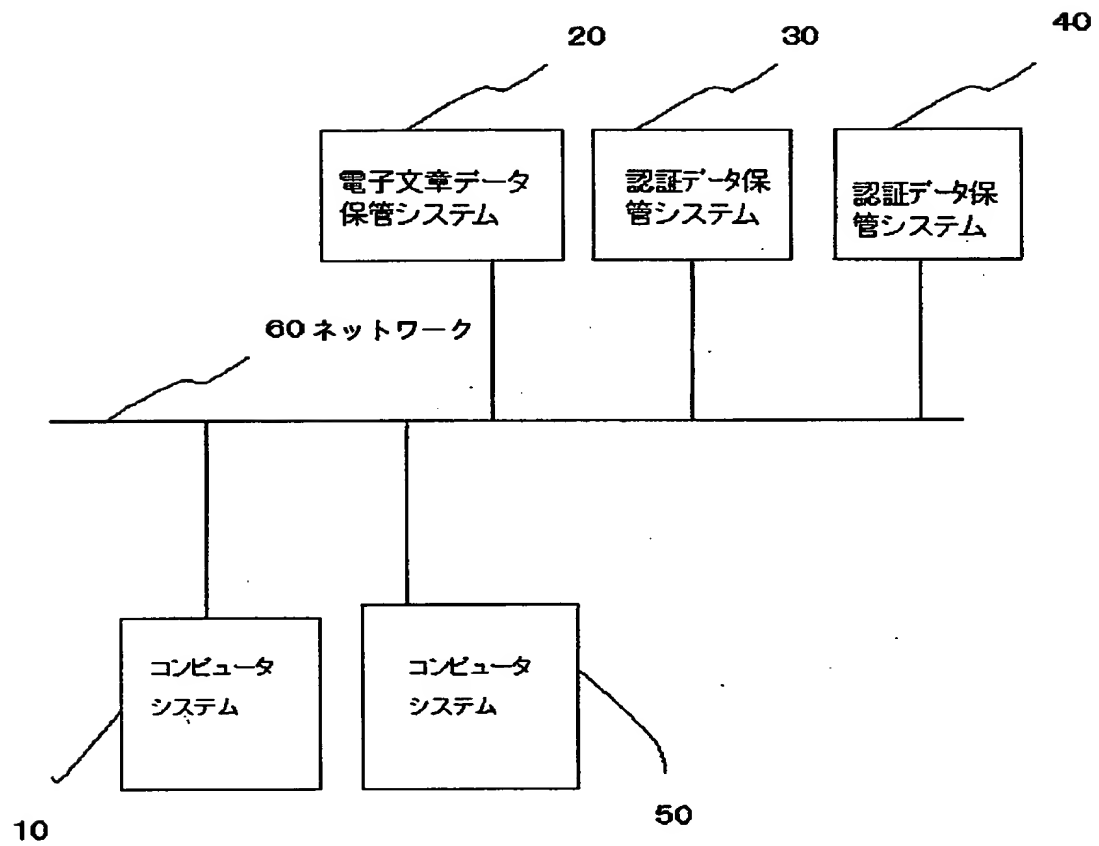
【符号の説明】

- 1 … 電子文章データ
- 1-1 … 文書管理の文書番号とそのバーコード
- 1-2 … 文書名
- 1-3 … 文
- 2 … 管理番号とそのバーコード
- 3, 4 … 認証者の認証データ
- 3-1, 4-1 … 認証イメージデータ
- 3-2, 4-2 … 管理番号と認証者の管理番号
- 3-3, 4-3 … 使用番号
- 10, 50 … コンピュータシステム
- 20 … 電子文章データ保管システム
- 21 … 文書管理ファイル
- 30, 40 … 認証データ保管システム
- 31, 41 … 認証管理ファイル
- 60 … ネットワーク

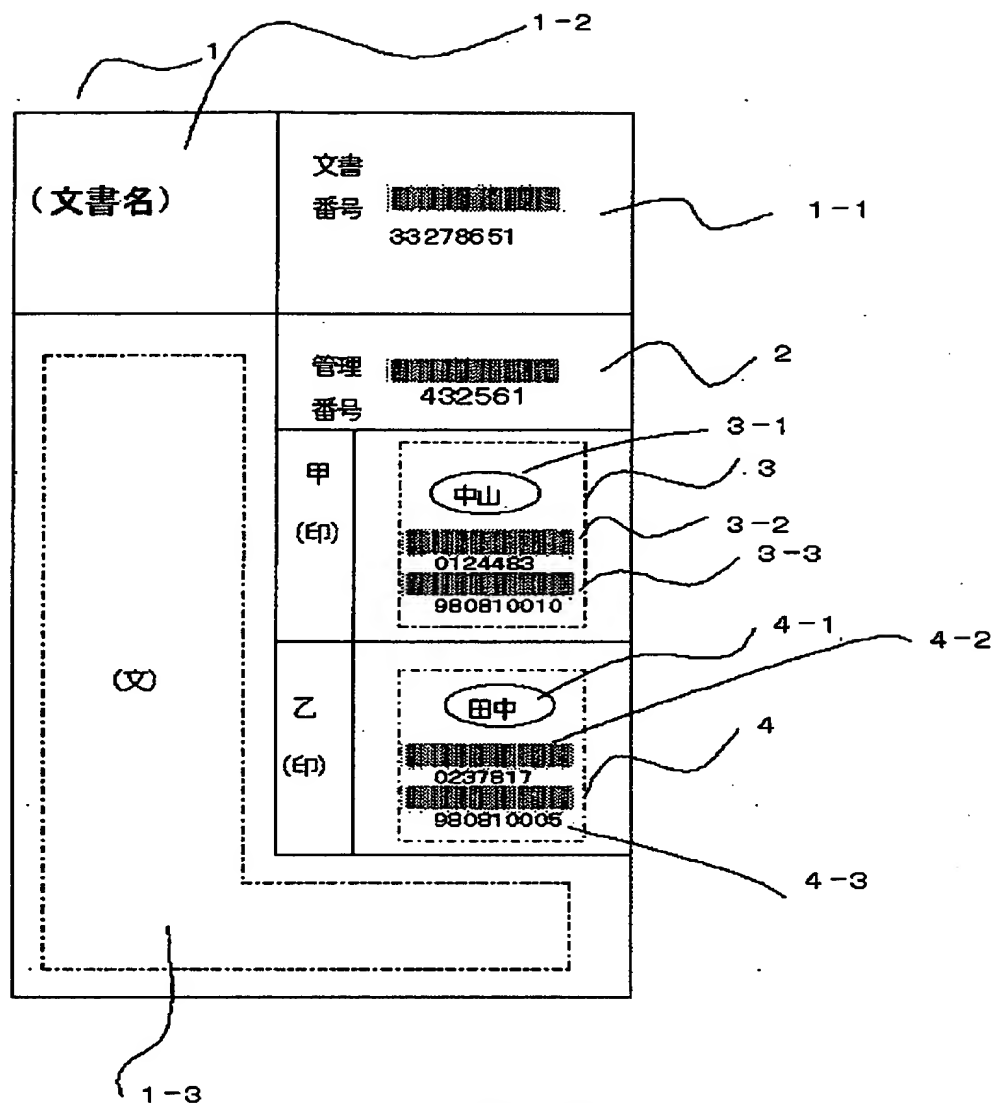
【書類名】

図面

【図 1】

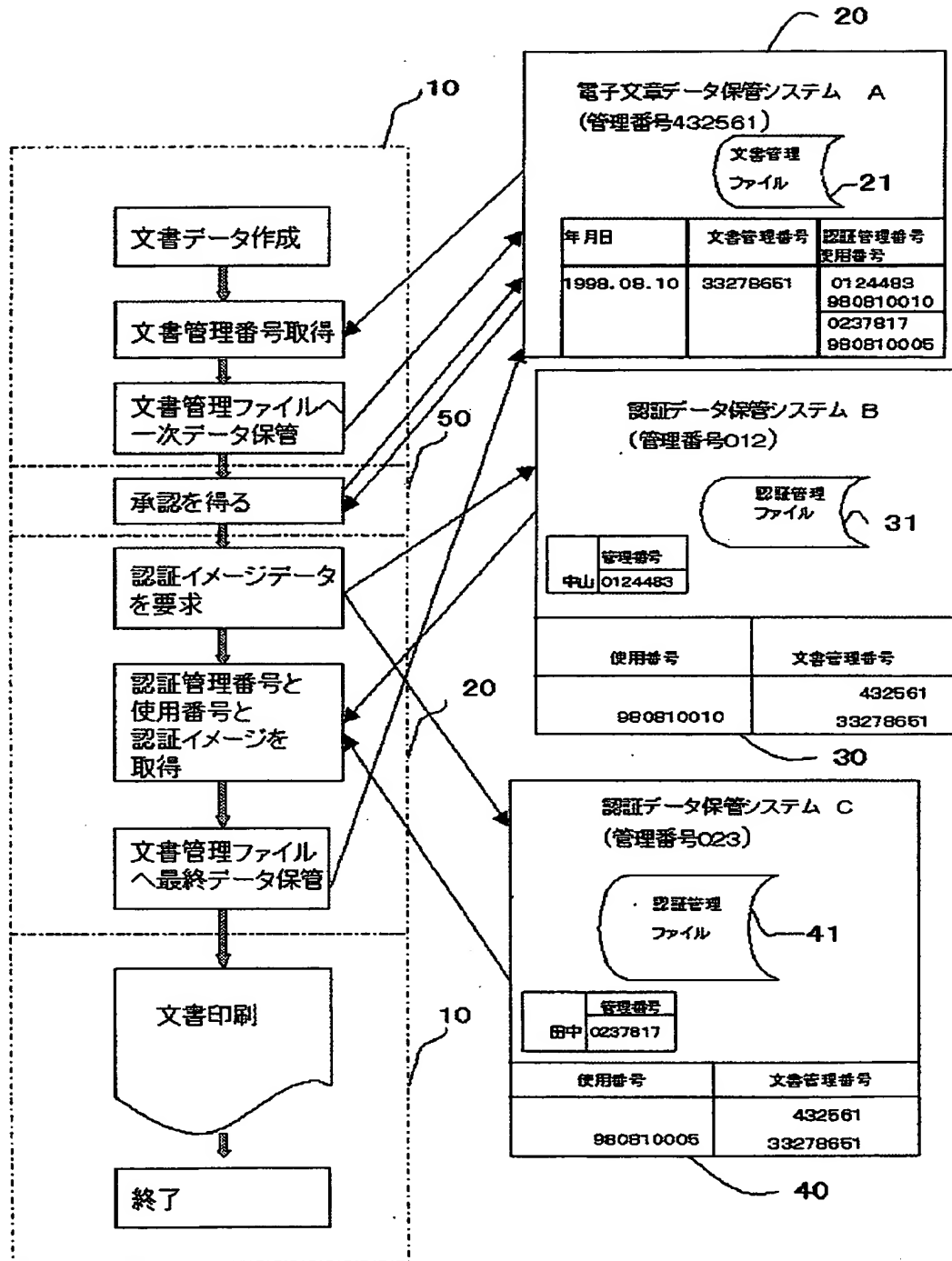


【図 2】



- 1…電子文章データ
- 1-1…文書管理の文書番号とそのバーコード
- 1-2…文書名
- 1-3…文
- 2…管理番号とそのバーコード
- 3, 4…認証者の認証データ
- 3-1, 4-1…認証イメージデータ
- 3-2, 4-2…管理番号と認証者の管理番号
- 3-3, 4-3…使用番号

【図 3】



【書類名】 要約書

【要約】

【課題】本発明は、認証の真贋の確認が容易でオープンかつ信頼性のある認証管理システム及び認証管理方法を提供することを課題とする。

【解決手段】認証としての印章やサインイメージの真贋の確認が容易なように認証としての印章やサインイメージの近傍にその認証の管理番号及び使用番号をバーコードで表示するとともに印字文書の中に文書の管理番号、及び保管機関のコードをバーコードで表示する。そしてオープンで信頼性のある認証管理システム及び認証管理方法の実現のため電子文章ファイルを保管する電子文章データ保管システムと個人や法人の印章やサインなどのイメージデータを認証データとして保管する認証データ保管システムにおいて、相互に認証データの管理番号と文章管理番号を保管及び管理する。

【選択図】 図2

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】
【識別番号】 000004237
【住所又は居所】 東京都港区芝五丁目7番1号
【氏名又は名称】 日本電気株式会社
【代理人】 申請人
【識別番号】 100097113
【住所又は居所】 東京都千代田区霞が関3-2-5 霞が関ビル35
階 霞が関ビル内郵便局 私書箱第2号 堀国際特
許事務所
【氏名又は名称】 堀 城之

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日
[変更理由] 新規登録
住 所 東京都港区芝五丁目7番1号
氏 名 日本電気株式会社